UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

SUSANNAH SMITH, individually and on behalf of all others similarly situated,	)	Case No.: _____
Plaintiff,	)	**CLASS ACTION COMPLAINT**
v.	)	
SUFFOLK UNIVERSITY,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Susannah Smith ("Plaintiff") brings this Class Action Complaint on behalf of herself, and all others similarly situated, against Defendant, Suffolk University ("Suffolk" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against Suffolk for its failure to properly secure and safeguard its students' sensitive personally identifiable information, including full names, Social Security Numbers, Driver's License numbers, state identification numbers, financial account information, and protected health information (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, damages, orders requiring Suffolk to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like this from

reoccurring in the future, and for Suffolk to provide identity theft protective services to Plaintiff and Class Members for their lifetimes, as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of Suffolk described herein.

2. In the course of enrolling, applying for and receiving financial aid, and receiving educational, medical, and other services from Suffolk, students provide their personal information to Suffolk. In turn, Suffolk comes into the possession of, and maintains files containing, the PII of its students.

3. On November 30, 2022, Suffolk notified its current and former students that their PII that had been stored on Suffolk's computer network had been accessed and removed by an unauthorized third-party (the "Data Breach").[1]

4. Based on the public statements of Defendant to date, a wide variety of PII was implicated in the Data Breach, including students' full names, Social Security Numbers, Driver's License numbers, state identification numbers, financial account information, and protected health information.[2]

5. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of cybercriminals.

6. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class

[1] Suffolk University Reports Data Breach Impacting Thousands of Current and Former Students, JDSUPRA (Dec. 7, 2022), https://www.jdsupra.com/legalnews/suffolk-university-reports-databreach-4061273/.

[2] Id.

Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

7. Plaintiff, on behalf of herself and all others similarly situated, allege claims for negligence, negligence per se, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard PII in Defendant's custody in order to prevent incidents like the Data Breach from reoccurring in the future and for Suffolk to provide identity theft protective services to Plaintiff and Class Members for their lifetimes.

PARTIES

8. Plaintiff Susannah is an adult who, at all relevant times, is a resident and citizen of the state of New Hampshire. Plaintiff was a student at Suffolk from approximately 2014 until she graduated in 2018. Plaintiff received a Data Breach notification informing her that her PII provided to Suffolk had been compromised in the Data Breach.

9. Since the announcement of the Data Breach, Plaintiff experienced fraudulent charges in her bank account in approximately early December 2023.

10. Plaintiff has been required to spend her valuable time monitoring her accounts and placing a freeze on her Social Security Number in an effort to detect and prevent any misuses of her PII—time which she would not have had to expend but for the Data Breach.

11. As a result of the Data Breach, Plaintiff will continue to be at heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

12. Moreover, because Plaintiff's health related PII was accessed in the Data Breach, Plaintiff has experienced and will continue to experience heightened anxiety knowing that her

health information has been exposed and is available for anyone to access on the dark web or other places on the Internet.

13. Defendant Suffolk University is a fully accredited private university and is located at 73 Tremont Street, Boston, MA 02108.

JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

15. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District and at all relevant times it has engaged in substantial business activities in Massachusetts.

16. Pursuant to 28 U.S.C. § 1391(b)(1) and (2), venue is proper in this District because this is where the Defendant has its principal place of business and where a substantial part of the events or omissions giving rise to the claims occurred.

COMMON FACTUAL BACKGROUND

17. Suffolk is a private university that offers bachelor's, master's, and doctoral degree programs in its Law School, College of Arts & Sciences, and Sawyer Business School.[3]

18. As of the Fall Semester of 2022, Suffolk has approximately 6,800 full-and parttime students and 86,000 active alumni.[4]

[3] Suffolk at a Glance, Suffolk University, https://www.suffolk.edu/about/suffolk-at-a-glance (last visited Jan. 4, 2023)

[4] Id.

19. While enrolling, applying for, and receiving financial aid, and receiving educational, medical, and other services from Suffolk, students provide their personal information, which includes, inter alia, full names, Social Security Numbers, Driver's License numbers, state identification numbers, financial account information, and protected health information to Suffolk.

20. In order to enroll in the university and receive the services that Suffolk offers, students must entrust their PII to Defendant, and in return, they reasonably expect that Defendant will safeguard their highly sensitive PII.

21. However, while Suffolk "prioritizes the privacy and security of all [its] students, faculty, staff, and alumni" and "take[s] [its] responsibility to safeguard data with which [it is] entrusted very seriously,"[5] Suffolk nevertheless employed inadequate data security measures to protect and secure the PII students entrusted to it, resulting in the Data Breach and compromise of Plaintiff's and Class Members' PII.

A. The Value of Private Information and Effects of Unauthorized Disclosure.

22. Suffolk was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

23. Suffolk also knew that a breach of its computer systems, and exposure of the PII stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

24. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

[5] William Woodring & Jamie Taris, 'Cybersecurity Incident' Impacts Current, Former Student Data, Suffolk Journal (Dec. 1, 2022), https://thesuffolkjournal.com/39536/news/cybersecurityincident-impacts-current-former-student-data/.

25. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[6]

26. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[7]

27. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[8]

28. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[9]

29. The ramifications of Suffolk's failure to keep Plaintiff and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches, "in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years.

---

[6] Brian Krebs, The Value of a Hacked Company, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[7] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

[8] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[9] Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime, Insurance Information Institute,https://www.iii.org/fact-statistic/facts-statistics-identity-theft-andcybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Dec. 29, 2022).

As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[10]

30. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

31. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's students especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

32. Based on the value of its students' PII to cybercriminals, Suffolk knew or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. Suffolk failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

B. Institutions of Higher Education are Particularly Vulnerable to Data Breaches.

33. Suffolk also knew or should have known that institutions of higher education have become prime targets for cybercriminals.

[10] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 4, 2023).

34. "Colleges and universities present a wealth of opportunities for cyber criminals. The market is enormous. There were 19.7 million college students in the U.S. in the fall of 2020, according to National Center for Education Statistics data."[11]

35. Universities house massive amounts of data. "The combination of employee and student personal and financial information, confidential data such as medical records, and commercially desirable research combined with the cultural openness of higher education has made Colleges and Universities prime targets" for cybercriminals.[12]

36. In conjunction with the large amounts of sensitive information colleges and universities possess, their computer networks further make them prime targets for cybercriminals because "[h]igher education institutions have historically underfunded cybersecurity efforts"[13] and "in contrast to corporations, higher education computer networks must allow for more open access to employees and students."[14]

37. Indeed, U.S. colleges and universities have been on high alert for cyberattacks. Between 2019 and 2020, Ransomware attacks on colleges doubled according to research by research by cybersecurity company BlueVoyant.[15] Further, the FBI issued a warning for higher education institutions in March 2021, informing them that cybercriminals had been targeting

---

[11] Peggy Bresnick, 4 Reasons Cyber Criminals Are Targeting Higher Education: Part 1, Fierce Education (Mar. 8, 2021), https://www.fierceeducation.com/best-practices/4-reasons-cybercriminals-are-targeting-higher-education-part-1.

[12] *Colleges and Universities are Prime Cyber Attack Targets*, Lamar University, https://www.lamar.edu/it-services-and-support/security/awareness/colleges-and-universities-areprime-cyberattack-targets.html (last visited Jan. 4, 2023).

[13] Emma Whiteford, *Cyberattacks Pose 'Existential Risk' To Colleges—And Sealed One Small College's Fate*, Forbes (Apr. 19, 2022), https://www.forbes.com/sites/emmawhitford/2022/04/19/cyberattacks-pose-existential-risk-tocolleges-and-sealed-one-small-colleges-fate/?sh=431590ea53c2.

[14] Lamar University, *supra* note 12.

[15] Lindsay McKenzie, Colleges a 'Juicy Target' for Cyberextortion, Inside Higher Ed (Mar. 19, 2021), https://www.insidehighered.com/news/2021/03/19/targeting-colleges-and-othereducational-institutions-proving-be-good-business.

institutions of higher education with ransomware attacks and later issued another warning in May 2022 warning that cyber actors continued to conduct attacks against U.S colleges and universities.[16]

38. Numerous high-profile colleges and universities have been victims of cyberattacks in recent months and years. For instance, in 2020, the University of California, San Francisco paid $1.14 million to hackers who encrypted and threatened to publish sensitive information stolen from the institution's School of Medicine and the University of Utah paid a ransom of $457,000.[17]

39. Likewise, in 2022 a handful of higher education institutions, such as North Carolina A&T State University, North Orange County Community College District, Ohlone Community College District, and Midland University all reported cyber-attacks.[18]

C. Suffolk Breached its Duty to Protect its Students PII.

40. On November 30, 2022, Suffolk reported the Data Breach to the attorney general offices of several states "after learning that an unauthorized party was able to access and remove certain files containing sensitive student information from the school's computer network."[19]

41. According to Suffolk, it discovered an unauthorized party gained access to its computer network on or about July 9, 2022.

42. After learning of the unauthorized access, Suffolk engaged cybersecurity experts to assist in an investigation. Suffolk completed the investigation on November 14, 2022 and concluded that the unauthorized third party gained access to and/or exfiltrated files containing

[16] *Increase in PYSA Ransomware Targeting Education Institutions*, Federal Bureau of Investigation (Mar. 16, 2021), https://www.ic3.gov/Media/News/2021/210316.pdf; Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums, Federal Bureau of Investigation (May 26, 2022), https://www.ic3.gov/Media/News/2022/220526.pdf.

[17] McKenzie, *supra* note 15.

[18] Whiteford, *supra* note 13.

[19] JDSUPRA, *supra* note 1.

students' PII. Suffolk President Marisa Kelly noted that the impacted data relates to students who enrolled in classes at Suffolk after June 2002.[20]

43. The students' PII exposed in the Data Breach includes students' including full names, Social Security Numbers, Driver's License numbers, state identification numbers, financial account information, and protected health information.[21]

44. On or about the same date that Suffolk reported the Data Breach to the attorney general offices of several states, Suffolk provided notice to Plaintiff indicating that documents containing her PII had been compromised and/or exfiltrated during the Data Breach.

45. Like Plaintiff, the Class Members received similar notices informing them that their PII was accessed and/or exfiltrated in the Data Breach.

46. While Suffolk has not released the total number of students affected by the Data Breach, approximately 36,000 people in Massachusetts alone were impacted by the Data Breach.[22]

47. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its students' PII.

D. FTC Guidelines Prohibit Suffolk from Engaging in Unfair or Deceptive Acts or Practices.

48. Suffolk is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

[20] Woodring & Taris, *supra* note 5.
[21] JDSUPRA, note 1.
[22] Id.

49. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

50. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[24]

51. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[25]

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Suffolk failed to properly implement basic data security practices. Suffolk's failure to employ reasonable and appropriate measures to protect against unauthorized access to student PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

---

[23] Start with Security – A Guide for Business, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[24] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[25] Id.

54. Suffolk was at all times fully aware of its obligations to protect the PII of students because of its position as an institution of higher education, which gave it direct access to reams of student PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Suffolk is Subject to, and Failed to Comply with, the GLBA.

55. The Gramm-Leach-Bliley Act ("GLBA"), states that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

56. A "financial institution" is defined as "any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12." 15 U.S.C. § 6809(3)(A). The GLBA contains no exemption for colleges or universities and both the FTC, and the Department of Education have made clear that Title IV institutions are subject to the GLBA.[26] As such, educational entities that engage in financial activities such as processing student loans, are required to comply.

57. "Nonpublic personal information" means "personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A)(i) – (iii). The PII involved in the Data Breach constitutes "nonpublic personal information" for purposes of the GLBA.

[26] National Association of College and University Counsel, NACUAlerts, FTC's Gramm-Leach Bliley Act Safeguards Rule: Guidelines for Compliance, Vol. 1, No 4. (May 16, 2003); Ted Mitchell, Undersecretary, U.S. Department of Education, Protecting Student Information (Jul. 1, 2016).

58. Upon information and belief, Suffolk is a Title IV institution that collects "nonpublic personal information", as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Suffolk was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801, et seq., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

59. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Suffolk violated the Safeguard Rule.

60. Suffolk failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

61. Suffolk's conduct resulted in a variety of failures to follow GLBA mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the

Data Breach demonstrates that Suffolk failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, adequate intrusion detection systems, regular reviews of audit logs and records, and other similar measures to protect the confidentiality of the PII it maintained in its data systems.

62. Had Suffolk implemented data security protocols, the consequences of the data exposure could have been avoided, or at least significantly reduced as the exposure could have been detected earlier, the amount of PII compromised could have been greatly reduced and affected consumers could have been notified—and taken protective/mitigating actions—much sooner.

F. Plaintiff and Class Members Suffered Damages.

63. The ramifications of Suffolk's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

64. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff and Class Members' PII has been diminished by its exposure in the Data Breach.

65. Plaintiff and Class Members are at substantial increased risk of suffering further identity theft and fraud or misuse of their PII as a result of the Data Breach. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant

increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[27]

66. Further, Plaintiff and Class Members have incurred and will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

67. Besides the monetary damage sustained in the event of identity theft, students may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[28]

68. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its students' PII.

69. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers.

70. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certainly impeding

[27] Stu Sjouwerman, 28 Percent of Data Breaches Lead to Fraud, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Jan. 4, 2023).

[28] Kathryn Parkman, How to Report identity Theft, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html.

injury flowing from fraud and identity theft posed by their PII being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their PII; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to it.

CLASS ALLEGATIONS

71. Plaintiff brings this class action on behalf of herself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

72. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States whose PII was compromised in the Suffolk University Data Breach which was announced on or about November 30, 2022 (the "**Class**").

73. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

74. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

75. *Numerosity*: Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including

but not limited to the files implicated in the Data Breach, but based on public information, the Class includes at a minimum 36,000 individuals.

76. *Commonality*: This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

77. *Typicality*: Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class are all former or current students of Defendant, each having their PII exposed and/or accessed by an unauthorized third party.

78. *Adequacy of Representation*: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

79. *Superiority*: This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action

presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

80. *Predominance*: Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

81. *Injunctive Relief*: Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

82. *Ascertainability*: Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendant's books and records.

//

//

//

//

//

//

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

83. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

84. Defendant owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' PII in Defendant's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

85. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that is routinely targeted by cyber-criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

86. Defendant breached the duties owed to Plaintiff and Class Members and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing;

(c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

87. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

88. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the PII;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of cybercriminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protected Plaintiff.

89. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

90. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

91. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by institutions such as Defendant or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

92. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach within the higher education sector.

93. Plaintiff and Class Members are customers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

94. Moreover, the harm that has occurred is the type of harm that the FTC was intended to guard against.

95. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

96. The GLBA states "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801(a).

97. Defendant violated the GLBA and the Safeguards Rule by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and disclosed and the foreseeable consequences of a data breach.

98. Plaintiff and Class Members are consumers within the class of persons the GLBA and the Safeguards Rule was intended to protect.

99. Moreover, the harm that has occurred is the type of harm that the GLBA and the Safeguards Rule was intended to guard against.

100. Defendant's violation of GLBA and the Safeguards Rule constitutes negligence per se.

101. As a direct and proximate result Defendant's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

102. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

103. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

104. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security

measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and remains at imminent risk that further compromises of her PII will occur in the future.

105. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure students' PII and to timely notify students of a data breach under the common law, Section 5 of the FTC Act, and GLBA; and

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure students' PII.

106. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect students' PII.

107. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach with Defendant. The risk of another such breach is real, immediate, and substantial. If another breach with Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

108. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

109. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose PII would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: January 31, 2023

Respectfully submitted,

/s/ Erica Mirabella
Erica C. Mirabella (BBO#676750)
MIRABELLA LAW, LLC
132 Boylston Street, 5thFloor
Boston, Massachusetts 02116
Telephone: 617-580-8270
Facsimile: 617-583-1905
erica@mirabellallc.com

Kevin Laukaitis*
LAUKAITIS LAW FIRM LLC
737 Bainbridge Street #155
Philadelphia, PA 19147
Ph: 215-789-4462
Email: klaukaitis@laukaitislaw.com

*Pro Hac Vice Application Forthcoming

Attorneys for Plaintiff and the Proposed Classes